METHOD OF OPERATING AN INTRUSION DETECTION SYSTEM ACCORDING TO A SET OF BUSINESS RULES

ABSTRACT

An intrusion detection system checks a list of business rules at predetermined update times, and determines whether any provision of the business rules has become newly operative since the last update time. Provisions of the business rules prescribe alterations to intrusion signatures, thresholds, actions, or weights that are appropriate to broader circumstances evident at the update time. Whenever a new provision is found to be operative, the effected signatures, thresholds, actions, or weights are altered accordingly.